WHAT IS CLAIMED IS:

1. A method for managing digital rights of software on a computer system, comprising:

encrypting at least a portion of an executable file to generate an encrypted executable file;

writing the encrypted executable file to a host location on the computer system during installation of software including the encrypted executable file; and

providing a loader for the encrypted executable file wherein the loader is operable to authenticate the encrypted executable file and cause the encrypted executable file to run on the computer system.

2. The method of claim 1 wherein the portion of the executable file comprises initial variables of the executable file.

3. The method of claim 1 further comprising executing the encrypted executable file.

4. The method of claim 3 wherein executing the encrypted executable file comprises:

authenticating the encrypted executable file;

writing the encrypted executable file to a memory location of the computer system;

decrypting the portion of the encrypted executable file; and

running the decrypted portion of the encrypted executable file.

5. The method of claim 4 wherein authenticating the encrypted executable file comprises confirming that rights in a rights document are satisfied.

6. The method of claim 5 wherein the rights document is appended to the encrypted executable file.

7. The method of claim 5 wherein confirming that rights in a rights document have been satisfied comprises determining whether the computer system is an authorized computer system on which the software is authorized to be installed.

8. The method of claim 5 wherein the rights document is an extensible markup language (XML) file.

9. The method of claim 4 wherein the authenticating, writing and decrypting are performed by the loader.

10. The method of claim 4 wherein authenticating the encrypted executable file comprises determining whether the encrypted executable file may be executed on the computer system.

11. The method of claim 4 wherein authenticating the encrypted executable file comprises accessing a central rights database via a communication pathway associated with the computer system.

12. The method of claim 11 further comprising managing the central rights database via a remotely located server.

13. The method of claim 12 wherein managing the central rights database comprises modifying usage rights of the software.

14. The method of claim 11 wherein the communication pathway includes an Internet connection.

15. The method of claim 1 further comprising tracking usage of the software.

16. The method of claim 15 wherein tracking usage of the software comprises gathering information about the usage of the software via a communication pathway associated with the computer system.

17. The method of claim 1 wherein the executable file can be executed via only the loader.

18. The method of claim 1 wherein the loader comprises software code specifically written to authenticate, load, decrypt and execute the encrypted executable file in a manner transparent to an end-user.

19. The method of claim 1 wherein the executable file comprises an executable binary file.

20. The method of claim 1 wherein the executable file comprises a header portion, a code portion and a data portion, and wherein encrypting at least a portion of an executable file comprises encrypting at least one of the code portion and the data portion.

21. A system for managing digital rights of software, comprising:

a computer including a communication device operable to communicate, via a communication pathway, with other electronic devices that are remote from the computer;

a remote authentication device in communication with the communication device via the communication pathway; and

software operable to be installed and run on the computer wherein the software comprises:

an executable file, and

an authentication loader program operable to authenticate and enable running of the executable file,

wherein the software is structured and arranged such that installation of the software is accomplished based on whether the remote authentication device permits the software

to be installed on the computer, and running of the software is accomplished based on whether the authentication loader program permits the software to be run on the computer.

22. The system of claim 21 wherein the computer further comprises a memory storage device operable to store digital information including the software, and a random access memory unit, the system further comprising a software installer program operable, based on whether the remote authentication device permits the software to be installed on the computer, to:

encrypt at least a portion of an executable file of the software, thereby generating an encrypted executable file,

append the authentication loader program to the encrypted executable file, and

write the authentication loader program and the encrypted executable file to the memory storage device of the computer.

23. The system of claim 21 wherein the computer further comprises a memory storage device operable to store digital information including the software, and a random access memory unit, and wherein the authentication loader program is operable to:

determine whether the executable file may be executed on the computer by authenticating the executable file,

read the executable file from the memory storage device of the computer,

identify a memory space in the random access memory unit for the executable file,

write the executable file to the memory space for execution, and

start the executable file of the software running.

24. The system of claim 23 wherein at least a portion of an executable file of the software is encrypted and wherein the authentication loader program is further operable to decrypt the portion of the executable file that is encrypted before starting the executable file of the software running.

25. The system of claim 24 wherein the authentication loader program starts the executable file of the software running immediately after decrypting the portion of the executable file that is encrypted.

26. The system of claim 23 wherein the remote authentication device is a server that manages a digital rights database wherein the authentication loader program includes code for causing the computer to access the remote authentication device to determine whether digital rights exist to run the software on the computer.

27. The system of claim 23 wherein the authentication loader program includes code for authenticating the executable file by confirming that rights in a rights document are satisfied.

28. The system of claim 27 wherein the rights document is appended to the executable file, and wherein the rights document is encrypted.

29. The system of claim 27 wherein the code for confirming that rights in the rights document are satisfied is operable to determine whether the computer is an authorized computer on which the software is authorized to be installed.

30. The system of claim 27 wherein the rights document includes an extensible markup language (XML) file.

31. The system of claim 21 wherein at least a portion of the executable file installed on the computer resides on the computer in encrypted format.

32. The system of claim 31 wherein the executable file is an executable binary file comprising a header portion, a code portion and a data portion, and wherein the portion of the executable file that resides on the computer in encrypted format comprises at least one of the code portion and the data portion.

33. The system of claim 21 wherein the remote authentication device includes a server that manages a digital rights database including digital rights relating to the software.

34. The system of claim 33 wherein the digital rights include a number of times a particular copy of the software is permitted to be installed.

35. The system of claim 34 wherein the digital rights database is accessed during installation of the software, and wherein the remote authentication device is operable to automatically decrement the number of times the particular copy of the software is permitted to be installed when the digital rights database is accessed during installation of the software.

36. The system of claim 33 wherein the digital rights include a number of times a particular installed copy of the software is permitted to be manipulated.

37. The system of claim 36 wherein the digital rights database is accessed by the authentication loader program during authentication of the executable file, and wherein the remote authentication device is operable to automatically decrement the number of times the particular installed copy of the software is permitted to be manipulated when the digital rights database is accessed during authentication of the executable file.

38. The system of claim 36 wherein manipulation of the software includes installation, execution, printing, duplication and modification of the software.

39. The system of claim 33 wherein the remote authentication device is operable to automatically modify the digital rights according to programmed criteria.

40. The system of claim 33 wherein the remote authentication device further comprises an interface through which the digital rights are modified by human intervention.

41. The system of claim 21 further comprising a software usage tracking unit wherein the software usage tracking unit is operable to gather and record information about usage of the software.

42. The system of claim 41 wherein the remote authentication device comprises the software usage tracking unit.

43. The system of claim 41 wherein the information about the usage of the software includes a number of times a particular copy of the software is installed.

44. The system of claim 41 wherein the information about the usage of the software includes identities of computers onto which a particular copy of the software is installed or is attempted to be installed.

45. The system of claim 41 wherein the information about the usage of the software includes a number of times a particular copy of the software is run.

46. The system of claim 21 wherein the communication pathway includes an Internet connection.

47. The system of claim 21 wherein each installation of the software is unique, such that a duplicated copy of installed software will not run properly.

48. The system of claim 21 wherein the remote authentication device permits an authorized backup copy of the software to function properly.

49. The system of claim 21 wherein the remote authentication device includes a server that manages a digital rights database wherein the digital rights database includes information about installation rights of individual copies of the software.

50. The system of claim 21 wherein the executable file can be executed only by the authentication loader program.

51. The system of claim 21 wherein the authentication loader program functions in a manner transparent to an end-user.

52. A method for managing digital rights during installation of software on a computer system, comprising:

accessing a digital rights database to determine whether the software is permitted to be installed on the computer system wherein an installation program performs the following based on whether the software is permitted to be installed on the computer system:

encrypting at least a portion of an executable file to produce an encrypted executable file;

appending a loader to the encrypted executable file; and

writing the loader and the encrypted executable file to a host storage location on the computer system.

53. The method of claim 52 further comprising tracking a number of times a particular copy of the software is installed.

54. The method of claim 52 further comprising logging an identity of the computer system onto which a particular copy of the software is installed or is attempted to be installed.

55. The method of claim 52 wherein the digital rights database includes information about installation rights of individual copies of the software.

56. The method of claim 52 further comprising duplicating the installation program wherein duplicated copies of the installation program do not function properly.

57. The method of claim 52 further comprising installing the software on the computer system in a manner unique from other copies of the software installed on other computer systems such that a copy of the software installed on a first computer system will not work properly on a second computer system.

58. The method of claim 52 further comprising generating an authorized backup copy of the software wherein the digital rights database permits the authorized backup copy of the software to function properly.

59. The method of claim 52 wherein accessing a digital rights database comprises communicating between the computer system and the digital rights database via a communication pathway associated with the computer system.

60. The method of claim 59 wherein the communication pathway includes an Internet connection.

61. The method of claim 52 wherein the digital rights database includes an encrypted computer file located on the computer system.

62. The method of claim 52 further comprising managing the digital rights database on a server remotely located from the computer system.

63. The method of claim 62 wherein managing the digital rights database comprises modifying digital rights of a particular copy of the software.

64. The method of claim 63 wherein the digital rights include a number of times the particular copy of the software may be installed.

65. The method of claim 64 wherein modifying the digital rights of a particular copy of the software comprises automatically decrementing the number of times the particular copy of the software may be installed when the central rights database is accessed during installation of the particular copy of the software.

66. The method of claim 63 further comprising automatically modifying the digital rights of the particular copy of the software when the digital rights database is accessed during installation of the particular copy of the software.

67. The method of claim 63 wherein the digital rights of the particular copy of the software are modified in the digital rights database via human intervention.

68. The method of claim 52 wherein the executable file can be executed via only the loader.

69. The method of claim 52 wherein the loader comprises software codes specifically written to authenticate, load, decrypt and execute the encrypted executable file in a manner transparent to an end-user.

70. The method of claim 52 wherein the executable file is an executable binary file.

71. The method of claim 52 wherein the executable file comprises a header portion, a code portion and a data portion, and wherein encrypting at least a portion of an executable file comprises encrypting at least one of the code portion and the data portion.

72. The method of claim 52 wherein encrypting at least a portion of an executable file comprises utilizing a 256-bit encryption algorithm to encrypt the portion of the executable file.

73. The method of claim 52 wherein the software further comprises the loader.

74. The method of claim 52 wherein encrypting at least a portion of an executable file comprises encrypting all of the executable file.

75. The method of claim 52 wherein encrypting at least a portion of an executable file comprises encrypting less than all of the executable file.